

2/Priority
4/12/87
K. Pannell
Docket No. 1614.1127/HJS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Mitsuru NAKAJIMA et al.

Group Art Unit:

Serial No.:

Examiner:

Filed: February 21, 2001

For: AUTHENTICATION METHOD, AUTHENTICATION SYSTEM....



**SUBMISSION OF CERTIFIED COPY OF PRIOR
FOREIGN APPLICATION IN ACCORDANCE WITH
THE REQUIREMENTS OF 37 C.F.R. § 1.55**

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

In accordance with the provisions of 37 C.F.R. § 1.55, the applicant(s) submit(s)
herewith a certified copy of the following foreign application(s):

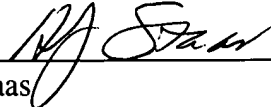
Japanese Patent Application No. 2000-256340
Filed: August 25, 2000

It is respectfully requested that the applicant(s) be given the benefit of the foreign filing
date, as evidenced by the certified papers attached hereto, in accordance with the requirements
of 35 U.S.C. § 119.

Respectfully submitted,
STAAS & HALSEY LLP

Date: February 21, 2001

By: _____


H. J. Staas
Registration No. 22,010

700 Eleventh Street, N.W., Suite 500
Washington, D.C. 20001
Telephone: (202) 434-1500
Facsimile: (202) 434-1501

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

JC929 U.S. PTO
09/788389
02/21/01

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日

Date of Application:

2000年 8月25日

出 願 番 号

Application Number:

特願2000-256340

出 願 人

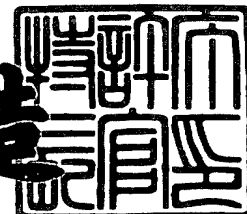
Applicant (s):

富士通株式会社

2000年12月 1日

特許庁長官
Commissioner,
Patent Office

及川耕造



出証番号 出証特2000-3101181

【書類名】 特許願

【整理番号】 0050522

【提出日】 平成12年 8月25日

【あて先】 特許庁長官 及川 耕造 殿

【国際特許分類】 G06F 15/20

【発明の名称】 認証処理方法、認証処理システム、決済方法、利用者装置及び認証処理を行うためのプログラムを格納した記憶媒体

【請求項の数】 10

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

【氏名】 中島 充

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

【氏名】 今嶋 佳明

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

【氏名】 半田 高敬

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

【氏名】 門間 仁

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

【氏名】 小高 敏裕

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

【氏名】 藤井 美香子

【特許出願人】

【識別番号】 000005223

【氏名又は名称】 富士通株式会社

【代理人】

【識別番号】 100070150

【住所又は居所】 東京都渋谷区恵比寿4丁目20番3号 恵比寿ガーデンプレイスタワー32階

【弁理士】

【氏名又は名称】 伊東 忠彦

【電話番号】 03-5424-2511

【手数料の表示】

【予納台帳番号】 002989

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9704678

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 認証処理方法、認証処理システム、決済方法、利用者装置及び
認証処理を行うためのプログラムを格納した記憶媒体

【特許請求の範囲】

【請求項 1】 取引を行う利用者間の認証に関する処理を行う認証処理システムにおける認証処理方法において、

前記利用者間で予定した取引に関して第 2 の利用者に照合キーを通知するステップと、

第 2 の利用者に通知された照合キーを第 2 の利用者より第 1 の利用者が受け取った後に、第 1 の利用者から通知される前記第 2 の利用者の照合キーの照合を行うステップとを有することを特徴とする認証処理方法。

【請求項 2】 請求項 1 記載の認証処理方法において、

前記認証処理システムは、照合キーを通知するステップに先だって、利用者の個人認証を行うことを特徴とする認証処理方法。

【請求項 3】 請求項 1 記載の認証処理方法において、

前記取引が予め設定された利用可能金額内であるか否かの判定を行うことを特徴とする認証処理方法。

【請求項 4】 請求項 1 記載の認証処理方法において、

前記取引が予め設定された取引条件に適合するか否かの判定を行うことを特徴とする認証処理方法。

【請求項 5】 請求項 1 記載の認証処理方法において、

前記照合キーを通知するステップは、双方の利用者に異なる照合キーを通知することを特徴とする認証処理方法。

【請求項 6】 請求項 1 記載の認証処理方法において、更に、

前記利用者間で予定した取引に関して第 1 の利用者に照合キーを通知するステップと、

第 1 の利用者に通知された照合キーを第 1 の利用者より第 2 の利用者が受け取った後に、第 2 の利用者から通知される前記第 1 の利用者の照合キーの照合を行うステップとを有することを特徴とする認証処理方法。

【請求項 7】 請求項 1 ないし 6 いずれか一項記載の認証処理方法における照合結果に基づいて、決済処理を行うことを特徴とする決済方法。

【請求項 8】 取引を行う利用者間の認証を行う認証処理システムにおいて、
前記利用者間で予定した取引に関して第 2 の利用者に照合キーを通知する通知手段と、

第 2 の利用者に通知された照合キーを第 2 の利用者より第 1 の利用者が受け取った後に、第 1 の利用者から通知される前記第 2 の利用者の照合キーの照合を行う照合手段とを有することを特徴とする認証処理システム。

【請求項 9】 取引を行う利用者間の認証に関する処理を行う利用者装置において、

該取引に関して各利用者に異なる照合キーを通知する認証処理システムに、前記利用者間で予定した取引に関する情報を送信する第 1 の送信手段と、

前記認証システムからの該取引に関する照合キーを受信する第 1 の受信手段と

利用者間で前記照合キーを通知し合った後に、照合キーの照合を行う認証処理システムに、相手から通知された相手側の照合キーを、送信する第 2 の送信手段と、

前記認証処理システムから照合結果を受信する第 2 の受信手段とを有することを特徴とする利用者装置。

【請求項 10】 取引を行う利用者間の認証に関する処理を行うためのプログラムを格納した記憶媒体であって、

コンピュータを動作させて、

該取引に関して各利用者に異なる照合キーを通知する認証システムに、前記利用者間で予定した取引に関する情報を送信する第 1 の送信手段と、

前記認証システムから該取引に関する照合キーを受信する第 1 の受信手段と、

利用者間で前記照合キーを通知し合った後に、照合キーの照合を行う認証処理システムに、相手から通知された相手側の照合キーを、送信する第 2 の送信手段と、

前記認証処理システムから照合結果を受信する第2の受信手段とを機能させるためのプログラムを格納したことを特徴とする記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、認証処理方法、認証処理システム、決済方法、利用者装置及び認証処理を行うためのプログラムを格納した記憶媒体に関する。

【0002】

【従来の技術】

対面販売において、購入者は、現金があれば、現金で決済するが、現金がない場合はクレジットカードで決済を行う。クレジットカードは、サインをするだけで、カード会社の加盟店から一定限度内の買物ができる。

【0003】

現在、クレジットカードは、現金を持ち歩かなくて済むことから、カード社会と言われる程に、普及している。

【0004】

また、昨今のインターネットの普及に伴い、インターネットを利用して、オンラインショッピングが行われている。この場合、決済手段として、会員番号、パスワード等を送信して、決済することも行われている。

【0005】

【発明が解決しようとする課題】

しかしながら、対面販売において、クレジットカードなどにより決済を行う場合、取り扱い加盟店の信憑性やカード番号のスキミングなど、安全性の面から問題が指摘されている。また、加盟店側においても、カード所有者が本人であるか否かの確認を行うことは困難であるという問題がある。

【0006】

また、オンラインショッピング等で、会員番号、パスワード等を、インターネット上に送信して決済することは、会員番号、パスワード等が傍受されるという危険があり、場合によっては、会員番号、パスワード等が盗まれ、本人に代わっ

て使用されるという問題がある。

【 0 0 0 7 】

本発明は、上記問題に鑑みなされたものであり、テンポラリな情報で認証を可能とし、安全で利便性の高い認証・決済手段を提供することを目的とするものである。

【 0 0 0 8 】

【課題を解決するための手段】

上記課題を解決するために、本件発明は、以下の特徴を有する課題を解決するための手段を採用している。

【 0 0 0 9 】

請求項 1 に記載された発明は、取引を行う利用者間の認証に関する処理を行う認証処理システムにおける認証処理方法において、前記利用者間で予定した取引に関して第 2 の利用者（例えば、図 1 における利用者 B）に照合キーを通知するステップと、第 2 の利用者に通知された照合キーを第 2 の利用者より第 1 の利用者（例えば、図 1 における利用者 A）が受け取った後に、第 1 の利用者から通知される前記第 2 の利用者の照合キーの照合を行うステップ（例えば、図 4 におけるステップ 2 6）とを有することを特徴とする。

【 0 0 1 0 】

請求項 1 記載の発明によれば、利用者間で予定した取引に関して第 2 の利用者に照合キーを通知し、更に、第 2 の利用者に通知された照合キーを第 2 の利用者より第 1 の利用者が受け取った後に、第 1 の利用者から通知される前記第 2 の利用者の照合キーの照合を行うことにより、テンポラリな情報で認証が可能となり、安全で利便性の高い認証を行うことができる。

【 0 0 1 1 】

請求項 2 に記載された発明は、請求項 1 記載の認証処理方法において、前記認証処理システムは、照合キーを通知するステップに先だって、利用者の個人認証を行う（例えば、図 2 におけるステップ 1 1、ステップ 1 2）ことを特徴とする。

【 0 0 1 2 】

請求項 2 記載の発明によれば、認証処理システムは、照合キーを通知するステップに先だって、利用者の個人認証を行うことにより、取引当事者は、相手の資格・当事者能力について心配することなく、安心して取引を行うことができる。

【 0 0 1 3 】

請求項 3 に記載された発明は、請求項 1 記載の認証処理方法において、前記取引が予め設定された利用可能金額内であるか否かの判定を行うことを特徴とする。

【 0 0 1 4 】

請求項 3 記載の発明によれば、取引が予め設定された利用可能金額内であるか否かの判定を行うことにより、取引当事者は、金額の心配をすることなく、安心して取引を行うことができる。

【 0 0 1 5 】

請求項 4 に記載された発明は、請求項 1 記載の認証処理方法において、前記取引が予め設定された取引条件に適合するか否かの判定を行うことを特徴とする。

【 0 0 1 6 】

請求項 4 記載の発明によれば、取引が予め設定された取引条件に適合するか否かの判定を行うことにより、取引当事者は、取引条件に関して心配をすることなく、安心して取引を行うことができる。

【 0 0 1 7 】

請求項 5 に記載された発明は、請求項 1 記載の認証処理方法において、前記照合キーを通知するステップは、双方の利用者に異なる照合キーを通知する（例えば、図 4 におけるステップ 2 1、ステップ 2 2）ことを特徴とする。

【 0 0 1 8 】

請求項 5 記載の発明によれば、照合キーを通知するステップは、双方の利用者に異なる照合キーを通知することにより、確実に認証を行うことができる。

【 0 0 1 9 】

請求項 6 に記載された発明は、請求項 1 記載の認証処理方法において、更に、前記利用者間で予定した取引に関して第 1 の利用者に照合キーを通知するステップと、第 1 の利用者に通知された照合キーを第 1 の利用者より第 2 の利用者が受

け取った後に、第2の利用者から通知される前記第1の利用者の照合キーの照合を行うステップとを有することを特徴とする。

【0020】

請求項6記載の発明によれば、更に、利用者間で予定した取引に関して第1の利用者に照合キーを通知するステップと、第1の利用者に通知された照合キーを第1の利用者より第2の利用者が受け取った後に、第2の利用者から通知される前記第1の利用者の照合キーの照合を行うステップとを有することにより、確実な認証を行うことができる。

【0021】

請求項7に記載された発明は、請求項1ないし6いずれか一項記載の認証処理方法における照合結果に基づいて、決済処理（例えば、図2におけるステップ19）を行うことを特徴とする。

【0022】

請求項7記載の発明によれば、請求項1ないし6いずれか一項記載の認証方法における照合結果に基づいて、決済処理を行うことができる。

【0023】

請求項8に記載された発明は、取引を行う利用者間の認証を行う認証処理システムにおいて、前記利用者間で予定した取引に関して第2の利用者に照合キーを通知する通知手段（例えば、図9における通知手段55）と、第2の利用者に通知された照合キーを第2の利用者より第1の利用者が受け取った後に、第1の利用者から通知される前記第2の利用者の照合キーの照合を行う照合手段（例えば、図9における照合手段57）とを有することを特徴とする。

【0024】

請求項8記載の認証処理システムは、請求項1ないし6に記載された認証方法に適した認証処理システムを規定したものである。

【0025】

請求項9に記載された発明は、取引を行う利用者間の認証に関する処理を行う利用者装置において、該取引に関して各利用者に異なる照合キーを通知する認証処理システムに、前記利用者間で予定した取引に関する情報を送信する第1の送

信手段（例えば、図 1 1 における送信手段 8 0）と、前記認証システムからの該取引に関する照合キーを受信する第 1 の受信手段（例えば、図 1 1 における受信手段 8 1）と、利用者間で前記照合キーを通知し合った後に、照合キーの照合を行う認証処理システムに、相手から通知された相手側の照合キーを、送信する第 2 の送信手段（例えば、図 1 1 における送信手段 8 0）と、前記認証処理システムから照合結果を受信する第 2 の受信手段（例えば、図 1 1 における受信手段 8 1）とを有することを特徴とする。

【 0 0 2 6 】

請求項 9 記載の利用者装置は、請求項 1 ないし 6 に記載された認証方法に適した利用者装置を規定したものである。

【 0 0 2 7 】

請求項 1 0 に記載された発明は、取引を行う利用者間の認証に関する処理を行うためのプログラムを格納した記憶媒体であって、コンピュータを動作させて、

該取引に関して各利用者に異なる照合キーを通知する認証システムに、前記利用者間で予定した取引に関する情報を送信する第 1 の送信手段と、前記認証システムから該取引に関する照合キーを受信する第 1 の受信手段と、利用者間で前記照合キーを通知し合った後に、照合キーの照合を行う認証処理システムに、相手から通知された相手側の照合キーを、送信する第 2 の送信手段と、前記認証処理システムから照合結果を受信する第 2 の受信手段とを機能させるためのプログラムを格納したことを特徴とする。

【 0 0 2 8 】

請求項 1 0 記載の取引を行う利用者間の認証に関する処理を行うためのプログラムを格納した記憶媒体は、請求項 1 ないし 6 に記載された認証方法に適した処理を行うためのプログラムを格納した記憶媒体を規定したものである。

【 0 0 2 9 】

【発明の実施の形態】

次に、本発明の実施の形態について図面と共に説明する。

【 0 0 3 0 】

本発明の認証及び決済システムの例を図 1 に示す。

【 0 0 3 1 】

図 1 は、利用者 A（第 1 の利用者、個人等）の端末 $10_1 \sim 10_N$ 、利用者 B（第 2 の利用者、店舗等）の端末 $20_1 \sim 20_M$ 、インターネット等の通信ネットワーク 30、アプリケーション・サービス・プロバイダ 40 から構成されている。また、プロバイダ 40 は、認証・決済システム 41、利用者 A データベース 42 及び利用者 B データベース 43 を有している。

【 0 0 3 2 】

利用者 A は、サービスの提供を受ける又は物を購入する本システムの利用者である。また、利用者 B は、利用者 A と取引を行う者で、サービスを提供する又は物を販売する本システムの利用者である。

【 0 0 3 3 】

利用者 A データベース 42 には、利用者 A の ID 番号、パスワード、決済情報及び商品を購入する資格の有無等の情報が格納され、利用者 B データベース 43 には、利用者 B の ID 番号、パスワード、決済情報及び商品を販売する資格に関する有無等の情報が格納されている。

【 0 0 3 4 】

認証・決済システム 41 は、後述するように、テンポラリな情報で、利用者 A また、認証・決済システム 41 は、利用者 A データベース 42 に格納されている利用者 A の ID 番号、パスワード、決済情報及び商品を購入する資格の有無等の情報及び利用者 B データベース 43 に格納されている利用者 B の ID 番号、パスワード、決済情報及び商品を販売する資格に関する有無等の情報に基づいて、利用者 A と利用者 B が、本サービスを受ける資格を有するか否かの資格チェック又はこれから行われる個別取引を行う資格を有するか否かの資格チェックを行う。

【 0 0 3 5 】

また、利用者 A の端末 $10_1 \sim 10_N$ 及び利用者 B の端末 $20_1 \sim 20_M$ は、固定端末でも携帯端末でもよい。ブラウザを搭載し、通信ネットワーク 30 を介して、アプリケーション・サービス・プロバイダ 40 に接続し、プロバイダ 40 が提供するウェブページを閲覧することができる。

【 0 0 3 6 】

図 2 を参照して、訪問販売の認証・決済を説明する。

【 0 0 3 7 】

訪問販売員（利用者 B）が玄関先に訪れた際に、自宅にいる人（利用者 A）の疑問である「この販売員と扱う商品の金額は妥当か」とか、訪問販売員の疑問である「この人は決済能力があるか」等を、携帯端末等を用いて解決できる。

【 0 0 3 8 】

つまり、以下に示す手順で認証を行い、それぞれが問題が無いことを確認した上で、商品を手渡すなどして取引を行う。

【 0 0 3 9 】

このシステムを利用する利用者 A と利用者 B とが、アプリケーション・サービス・プロバイダ 4 0 に加入していることが前提であり、利用者 A と利用者 B とが、個々に、プロバイダに登録する（S 1 0）。

【 0 0 4 0 】

次いで、利用者 B が利用者 A 宅を訪れ、利用者 A の玄関で対面したとき、個々に、端末（携帯端末等）を用いて、プロバイダ 4 0 に接続する。そのとき、利用者 A と利用者 B とは、個々に、ID 番号とパスワードを入力して、プロバイダから、本サービスが利用可能であることが認証される（S 1 1）。

【 0 0 4 1 】

次いで、利用者 A と利用者 B とが、それぞれ、取引可能か否かの取引資格の確認を行う（S 1 2）。例えば、利用者 A は、商品の購入をする資格を有しているか否かであり、利用者 B は、商品の販売をする資格を有しているか否かである。

【 0 0 4 2 】

プロバイダ 4 0 は、利用者 A データベース 4 2 及び利用者 B データベース 4 3 を参照して認証を行う。従って、商品の購入をする資格を有していない利用者 A は、この時点で以降の処理ができなくなる。また、商品の販売をする資格を有していない利用者 B は、この時点で以降の処理ができなくなる。

【 0 0 4 3 】

これにより、例えば、購買資力ない利用者 A、販売資格のない利用者 B を排除

できるので、安心して、取引ができる。

【 0 0 4 4 】

利用者 A が商品の購入をする資格を有しており、利用者 B が、商品の販売をする資格を有している場合は、取引キーの選定を行う（S 1 3）。

【 0 0 4 5 】

図 3 に取引ページの画面の例を示す。図 3 の取引ページの画面では、取引キー 1 ～取引キー N と、その取引キーに関連する利用者 A のボタン 5 0₁ ～ 5 0_N 及び利用者 B のボタン 5 1₁ ～ 5 1_N を有している。

【 0 0 4 6 】

利用者 A と利用者 B は、同じ、取引ページの画面を閲覧する。取引ページの画面には、利用可能な取引キーが示されている。

【 0 0 4 7 】

利用者 A と利用者 B は、互いに、どの取引キーを利用するかを決めて（S 1 3）、個々に、ボタンをクリックする。例えば、取引キー 2 を利用するのであれば、利用者 A はボタン 5 0₂ をクリックし、利用者 B はボタン 5 1₂ をクリックする。

【 0 0 4 8 】

ボタン 5 0₂ とボタン 5 1₂ が押されると、プロバイダ 4 0 から、利用者 A と利用者 B に対して、それぞれ、照合キーが通知され、それぞれ、利用者 A と利用者 B の画面に表示される（S 1 4）。

【 0 0 4 9 】

次いで、利用者 A と利用者 B とは、プロバイダ 4 0 から通知された照合キーを互いに、口頭等で通知する（S 1 5）。

【 0 0 5 0 】

次いで、利用者 A と利用者 B は、個々に、共通の取引番号（ここでは、取引キー 2 に対応した番号）に対して、相手から通知された、照合キーを入力する（S 1 6）。

【 0 0 5 1 】

前記プロバイダ 4 0 は、共通の取引番号と利用者 A と利用者 B からの二つの照

合キーが、それぞれ、前記個別取引に関して、前記プロバイダ 4 0 が通知した照合キーであるか否かを判定してキーの照合を行う（S 1 7）。

【 0 0 5 2 】

プロバイダ 4 0 は、判定した結果を利用者 A と利用者 B に通知する（S 1 8）。

【 0 0 5 3 】

照合が OK であれば、相手に問題が無いことが確認されたので、商品を手渡すなどして、取引を完了する。

【 0 0 5 4 】

次いで、プロバイダ 4 0 の決済機能等を利用して決済を行う（S 1 9）。

【 0 0 5 5 】

なお、必要であれば、利用者 A と利用者 B が、プロバイダ 4 0 から通知された照合キーを互いに通知するとき、決済に必要な金額等を通知・確認してもよい。

【 0 0 5 6 】

また、利用者 B は、個人であっても、企業であってもよい。

【 0 0 5 7 】

照合の方法（上記図 2 における S 1 4 ～ S 1 8）について、図 4 を用いて説明する。

【 0 0 5 8 】

上記図 3 において、取引キー 2 に関して、利用者 A がボタン 5 0₂ をクリックし、利用者 B が、ボタン 5 1₂ をクリックすると、利用者 A に個別キー（照合キー）（A）が通知され、利用者 B に個別キー（照合キー）（B）が通知される（S 2 1、S 2 2）。

【 0 0 5 9 】

個別キー（A）と個別キー（B）は、それぞれ異なるキーであり、取引キー 2 に関連する情報である。個別キー（A）と個別キー（B）とは、取引キー 2 の割り符に相当し、個別キー（A）と個別キー（B）とが合わされば、取引キー 2 が OK となるイメージである。

【 0 0 6 0 】

取引キー 2 は、利用者 A と利用者 B とで共有している。しかしながら、個別キー (A) は、利用者 A のみが知っている情報であり、個別キー (B) は、利用者 B のみが知っている情報である。

【 0 0 6 1 】

次いで、利用者 A と利用者 B とは、それぞれの個別キー (A) と個別キー (B) を交換する (S 2 3) 。

【 0 0 6 2 】

次いで、利用者 A と利用者 B は、プロバイダが提供する画面において、取引キー 2 に関して、相手から通知された、それぞれ入力する (S 2 5、S 2 6) 。

【 0 0 6 3 】

個別キーの入力は、例えば、S 2 6 に示すように、プロバイダ 4 0 が提供する、同じ画面を閲覧し、利用者 A と利用者 B は、それぞれ、画面の (A) 及び (B) に、相手から通知された個別キーを入力する。

【 0 0 6 4 】

なお、S 2 6 の「××××××」には、個別キー自体は、表示されない。

【 0 0 6 5 】

プロバイダ 4 0 は、利用者 A の個別キー (A) と取引相手から取得した個別キー (B) とが、取引キー 2 の割り符であるか否かを判定し、その結果を、利用者 A に通知し (S 2 7)、利用者 B の個別キー (B) と取引相手から取得した個別キー (A) とが、取引キー 2 の割り符であるか否かを判定し、その結果を、利用者 B に通知する (S 2 8) 。

【 0 0 6 6 】

符合すれば、目の前にいる人は、プロバイダ 4 0 が認証した、売買の資格を有する人であることが確認できたので、安心して取引を行うことができる。

【 0 0 6 7 】

本発明は、レストランでの活用も可能である。以下に、レストランの例を実施例として、図 5 ～図 7 を用いて説明する。

【 0 0 6 8 】

このシステムを利用するレストランの利用者とレストランとが、同じアプリケ

ーション・サービス・プロバイダに加入していることが前提であり、レストランの利用者とレストランとが、個々に、プロバイダに登録する。

図 5 (A) は、レストランの利用者が、プロバイダに登録し (S 3 0)、個別 ID とパスワードを払い出す (S 3 1) フローの例である。

図 5 (B) は、レストランが、プロバイダに登録し (S 3 2)、個別 ID とパスワードを払い出す (S 3 3) フローの例である。

図 6 は、取引を開始して、レストランの利用者が、レストランに行くまでの処理フローの例を示す。

【 0 0 6 9 】

レストランの利用者は、端末 (パソコン、携帯端末等) から、プロバイダに接続し、ID / パスワードを入力してログインを行う (S 4 0)。次いで、レストランの利用者は、取引種別 / 認証範囲を指定する (S 4 1)。具体的には、レストランの利用者が利用しようとする店の特定とサービスの提供受けたい又は物を購入したいとの申し出を行い、さらに、必要に応じて、レストランの利用者が受けたい保証の範囲を指定する。

【 0 0 7 0 】

このとき、レストランの利用者は、必要に応じて、取引の条件 (例えば、個室であるか否か又はランク等) を示すようにしてもよい。

【 0 0 7 1 】

取引キーを選択して、プロバイダから個別キー (A) を取得する (S 4 2)。

【 0 0 7 2 】

その後、プロバイダは、指定されたレストランに、取引依頼 (利用予約) があったことを、取引キーと共に、電子メール等で通知する (S 4 3)。

【 0 0 7 3 】

レストランでは、取引依頼 (利用予約) があったことを受けて (S 4 4)、プロバイダに接続し、ID / パスワードを入力してログインを行う (S 4 5)。次いで、通知された取引キーを選択又は入力して、プロバイダから個別キー (B) を取得する (S 4 6)。

【 0 0 7 4 】

図7は、レストランの受付カウンターでの処理フローの例を示す。

【0075】

レストランの利用者は、受付カウンターにおいて、口頭で、取引キーと個別キー（A）をレストランの受付の人に通知する（S50）。

【0076】

なお、取引キー（A）と個別キーのレストランへの通知は、電子メールで行われても良いし、レストランの利用者に代わって、プロバイダが行ってもよい。

【0077】

レストランの受付の人は、口頭等で、取引キーと個別キー（B）をレストランの利用者に通知する（S51）。

【0078】

その後、レストランとレストランの利用者は、別々に、プロバイダに接続し、ID／パスワードを入力してログインを行う（S52、S54）。

【0079】

レストランの利用者は、プロバイダが提供する画面で、取引キーと個別キー（B）と金額を入力する（S53）。同じく、レストランは、プロバイダが提供する画面で、取引キーと個別キー（A）と金額を入力する（S54）。

【0080】

プロバイダでは、取引キーに対して、それぞれの個別キーが照合するか否かを判定し、照合した結果を、金額と共に、レストランとレストランの利用者に通知する（S56）。

【0081】

レストランとレストランの利用者の端末には、照合された結果が表示される（S57、S58）。

【0082】

この結果、予約したレストランの利用者は、所望した条件のサービスを受けることができる。

【0083】

なお、金額の入力欄を設け無くてもよい。また、金額の入力欄に記入しなくて

も、認証を行うようにしてもよい。

【 0 0 8 4 】

上述の通り、プロバイダ 4 0 は、共通の取引キーと利用者 A と利用者 B からの二つの識別キー（個別キー（A）と個別キー（B））が、符号するか否かで、照合している。

【 0 0 8 5 】

これには、二つのタイプがある。

【 0 0 8 6 】

一つは、図 8（A）に示したように、共通の取引キーに対して、プロバイダが、個別キー（A）と個別キー（B）を払い出す場合で、上述の例は、図 8（A）の例に相当する。

【 0 0 8 7 】

一方、図 8（B）は、個別キー（A）と個別キー（B）とに、それぞれ、ユニークな情報を設定し、共通の取引キーとしては、個別キー（A）と個別キー（B）とから生成されるキーを用いる。

【 0 0 8 8 】

ユニークな情報として、認証に使用する個別 ID を用いることも可能である。しかしながら、セキュリティ上のことを考慮して、認証に使用する個別 ID 自体でなく、例えば、ログオン時に、払いだされたテンポラリな個別 ID を使用するようにしてもよい。

【 0 0 8 9 】

共通の取引キー自体は、取引を識別できれば良いので必ずしも、秘密にする必要も無いが、他の取引キーと区別するために、独自の取引キーを生成することが好ましい。

【 0 0 9 0 】

例えば、共通の取引キーとして、単に、個別キー（A）と個別キー（B）とを並べたものでも良いし、個別キー（A）と個別キー（B）を基に、何らかの論理演算処理を施したものでもよい。

【 0 0 9 1 】

例えば、個別キー（A）が「1 2 3 4」であり、個別キー（B）が「5 6 7 8」の場合、共通の取引キーとして、単に並べた、「1 2 3 4 5 6 7 8」としてもよい。また、共通の取引キーとして、両者を掛け算した、「7 0 0 6 6 5 2」としてもよい。また、個別キー（A）と個別キー（B）と2進数の論理演算でもよい。

【0 0 9 2】

図 8（B）では、プロバイダは、個別キーの払い出しの処理が不要となる。

【0 0 9 3】

なお、本発明は、ホテル予約システムでの活用も可能である。

【0 0 9 4】

例えば、プロバイダに加入しているホテルを予約する場合、インターネット接続可能な携帯端末（電話）を通じて、事前に予約し、照合キー A（予約番号）を取得する。予約先のホテルでは、予約者の予約を確認し、照合キー B（確認番号）を予約者に通知する。

【0 0 9 5】

予約者は、確認番号を入力することでホテルに対する照合を完了する。一方、ホテルは、利用時に予約者から予約番号を確認し利用者本人を確認するとともに、決済を確認する。

【0 0 9 6】

さらに、本発明は、遊園地・映画館等での入場予約システムとして活用できる。

【0 0 9 7】

例えば、プロバイダに加盟している遊園地などの施設を利用する場合は、事前に予約番号を取得し、内部的に情報照合を終えておくことで、予約先の施設に入園する際に予約番号を施設側パソコンなどから入力することで入場を可能とする。

と利用者 B 間の認証を行い、安全で利便性の高い認証・決済手段を提供する。

【0 0 9 8】

図 9 に認証・決済システム 4 1 における主要な機能ブロックの例を示す。

【 0 0 9 9 】

決済手段 5 4 は、認証と取引が行われた場合、当該取引に関して決済を行う。

【 0 1 0 0 】

通知手段 5 5 は、取引に関して、双方の利用者に異なる照合キーを通知し、照合の結果、取引に係る通知等を行う。

【 0 1 0 1 】

受取手段 5 6 は、取引に関して各利用者に通知した照合キーであって、利用者間で交換した照合キー等を受け取る。

【 0 1 0 2 】

照合手段 5 7 は、一方の利用者に通知された照合キーを他方の利用者が受け取った後に、他方の利用者から通知される一方の利用者の照合キーに係る照合、他方の利用者に通知された照合キーを一方の利用者が受け取った後に、一方の利用者から通知される他方の利用者の照合キーに係る照合等を行う。

【 0 1 0 3 】

資格チェック手段 5 8 は、本システムを利用する資格が有るか否か、取引を行う資格が有るか否かのチェック等を行う。

【 0 1 0 4 】

図 1 0 に、サーバ 4 0 のハードウェア構成の例を示す。

【 0 1 0 5 】

図 1 0 では、キーボード、ポインティングデバイス等の入力装置 6 1、CPU (Central Processing Unit : 中央処理装置) 6 2、ROM (Read only memory) 6 3、RAM (Random Access memory) 6 4、通信ネットワーク 2 0 とインタフェースをとる通信 IF (インタフェース) 6 5、内部バス 6 6、外付けの HDD (Hard Disk Drive)、プリンタ、スキャナとインタフェースを取る IF (インタフェース) 6 7、HDD 6 8、FD (Floppy Disk) の書込み及び読出しを行う FDD (Floppy Disk Drive) 6 9、CD-ROM の読み込みを行う CD-ROM ドライブユニット 7 0、ディスプレイ 7 4 の表示コントローラ 7 1 から構成されている。

【0106】

ハードウェア自体の機能は、周知であるので説明を省略する。

【0107】

本発明の認証処理を行うためのプログラムを記録した記憶媒体を作成し、この記録媒体から、本発明の認証処理を行うためのプログラムを読み出して、CPU 62に実行させて、認証処理を行うことができる。

【0108】

なお、本発明の認証処理を行うためのプログラムを記録した記憶媒体は、フロッピディスク、ハードディスク、光ディスク（CD-ROM、CD-R、CD-R/W、DVD-ROM、DVD-RAMなど）、光磁気ディスク、メモ리카ードなどであってもよい。

【0109】

図11に利用者端末（A、B）における主要な機能ブロックの例を示す。

【0110】

図11では、送信手段80、受信手段81、入力手段82及び出力手段83から構成されている。

【0111】

送信手段80は、利用者間で予定した取引に関する情報をサーバに送信し、更に、利用者間で照合キーを交換して得た相手側の照合キー等を送信する。

【0112】

受信手段81は、サーバからの取引に関する照合キーを受信し、更に、照合結果等を受信する。

【0113】

入力手段82は、認証・決済処理に必要な事項を入力する。例えば、ID、パスワード、照合キー等の入力を行う。

【0114】

出力手段83は、認証・決済処理において、利用者端末に送られた情報を表示する。

【0115】

以上の通り、本発明の実施の形態又は実施例によれば、カード又は現金を所持する必要がなくなる。

【 0 1 1 6 】

ところで、現実社会におけるカード又は現金の支払いにおいては、常にカード又は現金を所持していなければならず、紛失、盗難の可能性が高い。また、カード又は現金を所持していない場合は、買い物又はサービスを受けられないなど利便性が悪い。また、カード利用時には、カード番号漏洩など安全性（セキュリティ）、信頼性においても少なからず問題が残っている。

【 0 1 1 7 】

本発明では、カード又は現金を所持する必要がないことにより、上記問題が無くなる。

【 0 1 1 8 】

上述の如く、本発明によれば、テンポラリな情報で認証を可能とし、安全で利便性の高い認証・決済手段を提供することができる。

【 0 1 1 9 】

また、プロバイダの加入情報をベースに認証し合うことにより、カード又は現金を所持することなく、決済処理が可能となり、カード又は現金を所持上の問題は解消される。

【 0 1 2 0 】

また、カード又は現金を所持しなくとも、リアルタイムの取引が可能となり、安全に各種対面販売取引を行うことが可能となる。

【 0 1 2 1 】

次に、発明の態様を付記として示す。

（付記 1）取引を行う利用者間の認証に関する処理を行う認証処理システムにおける認証処理方法において、

前記利用者間で予定した取引に関して第 2 の利用者に照合キーを通知するステップと、

第 2 の利用者に通知された照合キーを第 2 の利用者より第 1 の利用者が受け取った後に、第 1 の利用者から通知される前記第 2 の利用者の照合キーの照合を行

うステップとを有することを特徴とする認証処理方法。(1)

(付記2) 付記1記載の認証処理方法において、

前記認証処理システムは、照合キーを通知するステップに先だって、利用者の個人認証を行うことを特徴とする認証処理方法。(2)

(付記3) 付記1記載の認証処理方法において、

前記取引が予め設定された利用可能金額内であるか否かの判定を行うことを特徴とする認証処理方法。(3)

(付記4) 付記1記載の認証処理方法において、

前記取引が予め設定された取引条件に適合するか否かの判定を行うことを特徴とする認証処理方法。(4)

(付記5) 付記1記載の認証処理方法において、

前記照合キーを通知するステップは、双方の利用者に異なる照合キーを通知することを特徴とする認証処理方法。(5)

(付記6) 付記1記載の認証処理方法において、

前記利用者は、前記認証処理システムが提供する同じ画面を閲覧し、それぞれの端末で表示されている画面上で、認証に必要な情報を選択又は入力することを特徴とする認証処理方法。

【0122】

なお、付記6に記載された発明によれば、利用者は、同じウェブページを閲覧しながら、認証を行うことができるので、確実にしかも簡便に行うことができる。

(付記7) 付記1記載の認証処理方法において、更に、

前記利用者間で予定した取引に関して第1の利用者に照合キーを通知するステップと、

第1の利用者に通知された照合キーを第1の利用者より第2の利用者が受け取った後に、第2の利用者から通知される前記第1の利用者の照合キーの照合を行うステップとを有することを特徴とする認証処理方法。(6)

(付記8) 付記1記載の認証処理方法において、

前記利用者の照合キーは、前記利用者を特定するユニークな情報であることを

特徴とする認証処理方法。

【 0 1 2 3 】

付記 8 に記載された発明によれば、利用者の照合キーとして、利用者を特定するユニークな情報を用いることにより、プロバイダ等の処理負担を減少させることができる。

(付記 9) 付記 1 ないし 8 いずれか一項記載の認証処理方法における照合結果に基づいて、決済処理を行うことを特徴とする決済方法。(7)

(付記 1 0) 取引を行う利用者間の認証を行う認証処理システムにおいて、前記利用者間で予定した取引に関して第 2 の利用者に照合キーを通知する通知手段と、

第 2 の利用者に通知された照合キーを第 2 の利用者より第 1 の利用者が受け取った後に、第 1 の利用者から通知される前記第 2 の利用者の照合キーの照合を行う照合手段とを有することを特徴とする認証処理システム。(8)

(付記 1 1) 取引を行う利用者間の認証に関する処理を行う利用者装置において、

該取引に関して各利用者に異なる照合キーを通知する認証処理システムに、前記利用者間で予定した取引に関する情報を送信する第 1 の送信手段と、

前記認証システムからの該取引に関する照合キーを受信する第 1 の受信手段と

、利用者間で前記照合キーを通知し合った後に、照合キーの照合を行う認証処理システムに、相手から通知された相手側の照合キーを、送信する第 2 の送信手段と、

前記認証処理システムから照合結果を受信する第 2 の受信手段とを有することを特徴とする利用者装置。(9)

(付記 1 2) 取引を行う利用者間の認証に関する処理を行うためのプログラムを格納した記憶媒体であって、

コンピュータを動作させて、

該取引に関して各利用者に異なる照合キーを通知する認証システムに、前記利用者間で予定した取引に関する情報を送信する第 1 の送信手段と、

前記認証システムから該取引に関する照合キーを受信する第 1 の受信手段と、利用者間で前記照合キーを通知し合った後に、照合キーの照合を行う認証処理システムに、相手から通知された相手側の照合キーを、送信する第 2 の送信手段と、

前記認証処理システムから照合結果を受信する第 2 の受信手段とを機能させるためのプログラムを格納したことを特徴とする記憶媒体。(10)

【発明の効果】

上述の如く本発明によれば、次に述べる種々の効果を奏することができる。
請求項 1 記載の発明によれば、利用者間で予定した取引に関して第 2 の利用者に照合キーを通知し、更に、第 2 の利用者に通知された照合キーを第 2 の利用者より第 1 の利用者が受け取った後に、第 1 の利用者から通知される前記第 2 の利用者の照合キーの照合を行うことにより、テンポラリな情報で認証が可能となり、安全で利便性の高い認証を行うことができる。

【0124】

請求項 2 記載の発明によれば、認証処理システムは、照合キーを通知するステップに先だって、利用者の個人認証を行うことにより、取引当事者は、相手の資格・当事者能力について心配することなく、安心して取引を行うことができる。

【0125】

請求項 3 記載の発明によれば、取引が予め設定された利用可能金額内であるか否かの判定を行うことにより、取引当事者は、金額の心配をすることなく、安心して取引を行うことができる。

【0126】

請求項 4 記載の発明によれば、取引が予め設定された取引条件に適合するか否かの判定を行うことにより、取引当事者は、取引条件に関して心配をすることなく、安心して取引を行うことができる。

【0127】

請求項 5 記載の発明によれば、照合キーを通知するステップは、双方の利用者に異なる照合キーを通知することにより、確実に認証を行うことができる。

【0128】

請求項 6 記載の発明によれば、更に、利用者間で予定した取引に関して第 1 の利用者に照合キーを通知するステップと、第 1 の利用者に通知された照合キーを第 1 の利用者より第 2 の利用者が受け取った後に、第 2 の利用者から通知される前記第 1 の利用者の照合キーの照合を行うステップとを有することにより、確実な認証を行うことができる。

【 0 1 2 9 】

請求項 7 記載の発明によれば、請求項 1 ないし 6 いずれか一項記載の認証方法における照合結果に基づいて、決済処理を行うことができる。

【 0 1 3 0 】

請求項 8 記載の発明によれば、請求項 1 ないし 6 に記載された認証方法に適した認証処理システムを提供することができる。

【 0 1 3 1 】

請求項 9 記載の発明によれば、請求項 1 ないし 6 に記載された認証方法に適した利用者装置を提供することができる。

【 0 1 3 2 】

請求項 1 0 記載の発明によれば、請求項 1 ないし 6 に記載された認証方法に適した処理を行うためのプログラムを格納した記憶媒体を提供することができる。

【図面の簡単な説明】

【図 1】

本発明の認証及び決済システムの例を説明するための図である。

【図 2】

認証及び決済の処理フローの例である。

【図 3】

取引ページ画面例である。

【図 4】

取引の照合を説明するための処理フローの例である。

【図 5】

前処理の処理フローの例である。

【図 6】

取引を開始して、レストランの利用者が、レストランに行くまでの処理フローの例である。

【図 7】

レストランの受付カウンターでの処理フローの例である。

【図 8】

取引の照合を説明するための図である。

【図 9】

認証・決済システムにおける主要な機能ブロックの例を説明するための図である。

【図 1 0】

プロバイダのハードウェア構成の例を説明するための図である。

【図 1 1】

利用者端末（A、B）における主要な機能ブロックの例を説明するための図である。

【符号の説明】

1 0₁ ~ 1 0_N 利用者 A（サービスの提供を受ける又は物を購入する第 1 の利用者）端末

2 0₁ ~ 2 0_M 利用者 B（サービスを提供する又は物を販売する第 2 の利用者）端末

3 0 通信ネットワーク

4 0 アプリケーション・サービス・プロバイダ

4 1 認証・決済システム

4 2 利用者 A のデータベース

4 3 利用者 B のデータベース

5 4 決済手段

5 5 通知手段

5 6 受取手段

5 7 照合手段

5 8 資格チェック手段

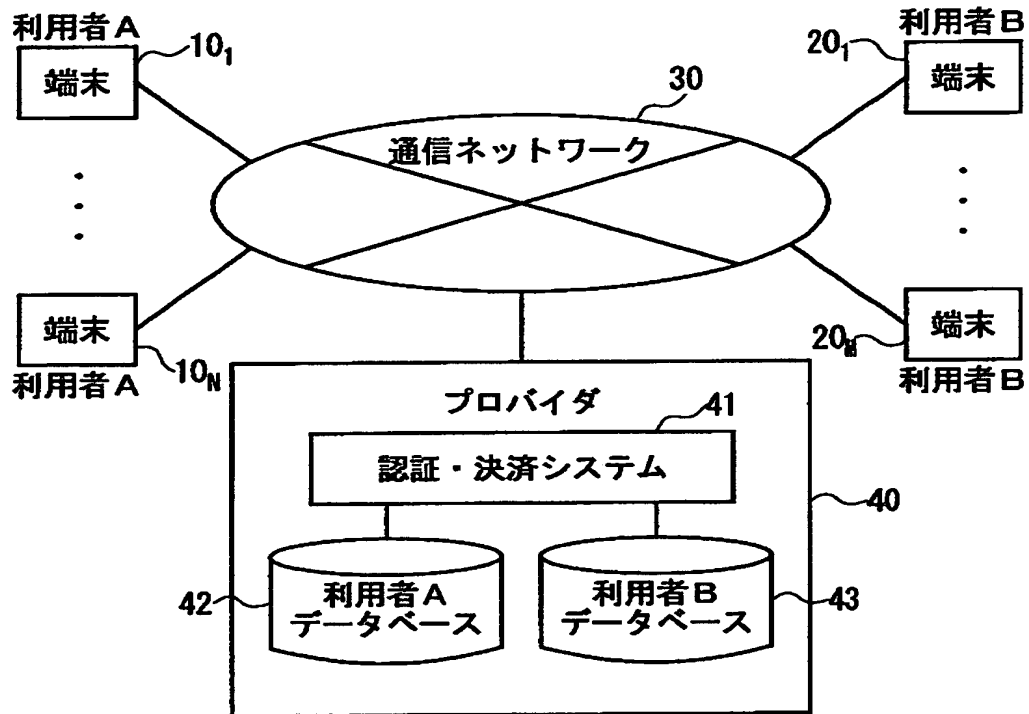
- 6 1 入力装置
- 6 2 C P U
- 6 3 R O M
- 6 4 R A M
- 6 5 通信 I F
- 6 7 I F
- 6 8 H D D
- 6 9 F D D
- 7 0 C D - R O M ドライブユニット
- 7 1 表示コントローラ
- 7 2 F D
- 7 3 C D - R O M
- 7 4 ディスプレイ
- 8 0 送信手段
- 8 1 受信手段
- 8 2 入力手段
- 8 3 出力手段

【書類名】

図面

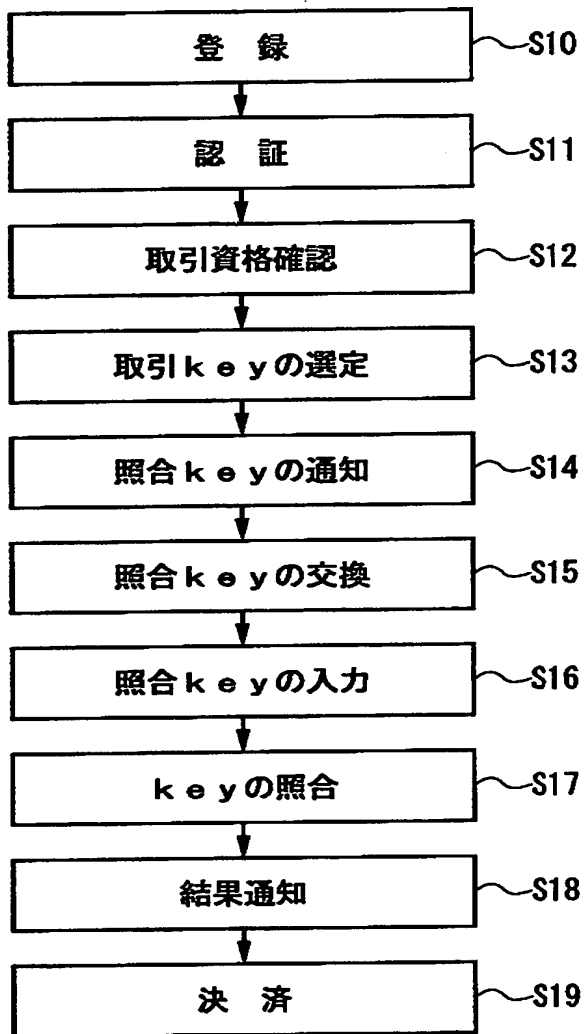
【図 1】

本発明の認証及び決済システムの例を説明するための図



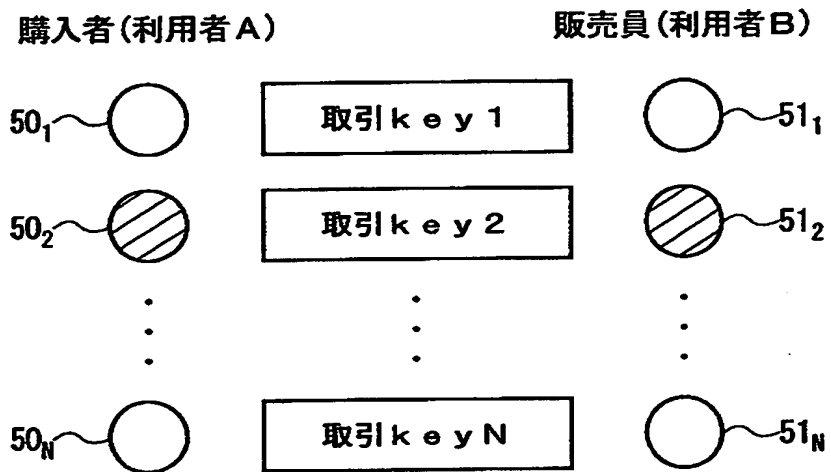
【図 2】

相互認証及び決済の処理フローの例



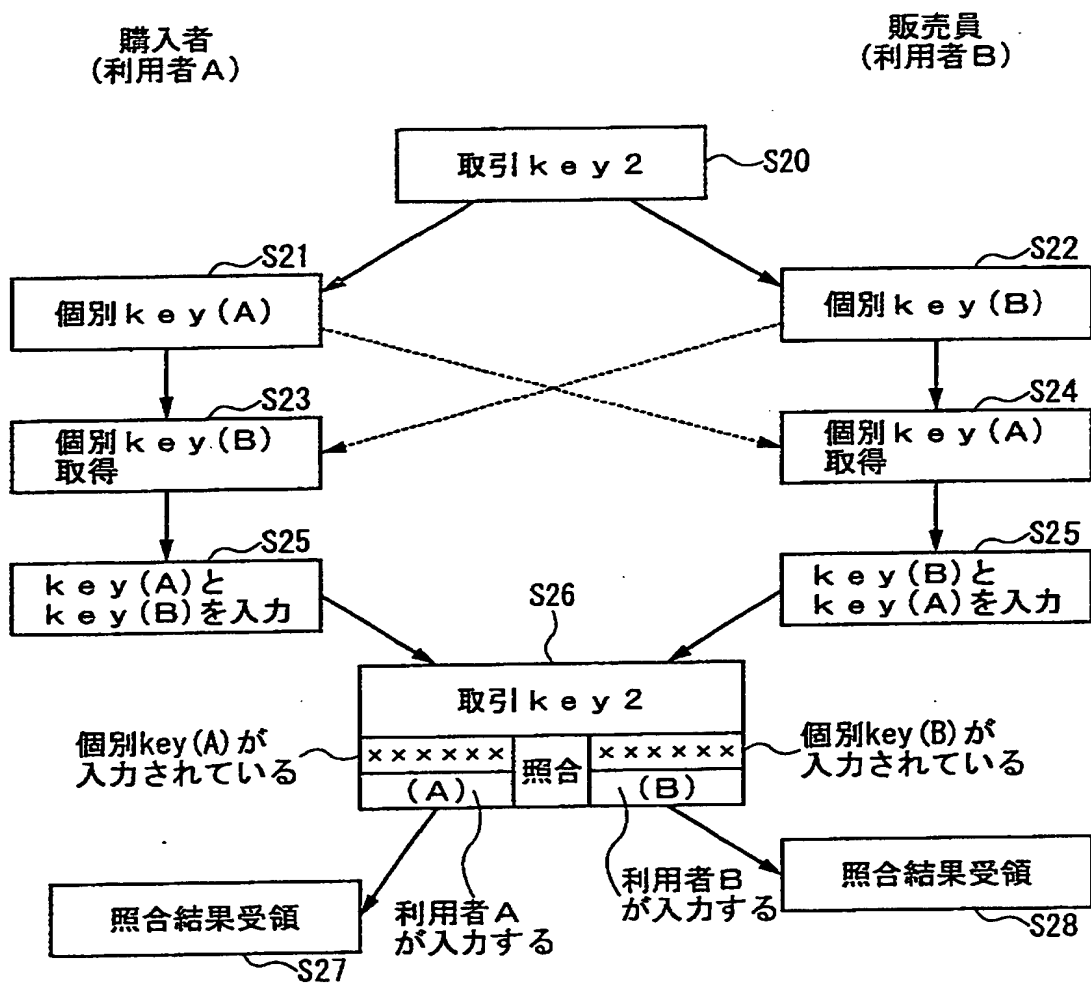
【図 3】

取引ページ画面



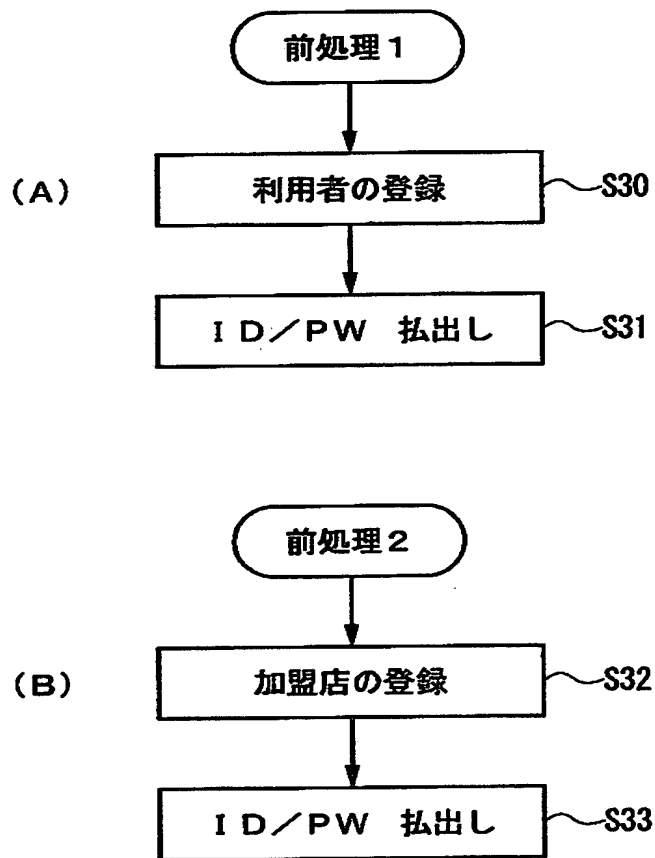
【図 4】

取引の照合を説明するための処理フローの例



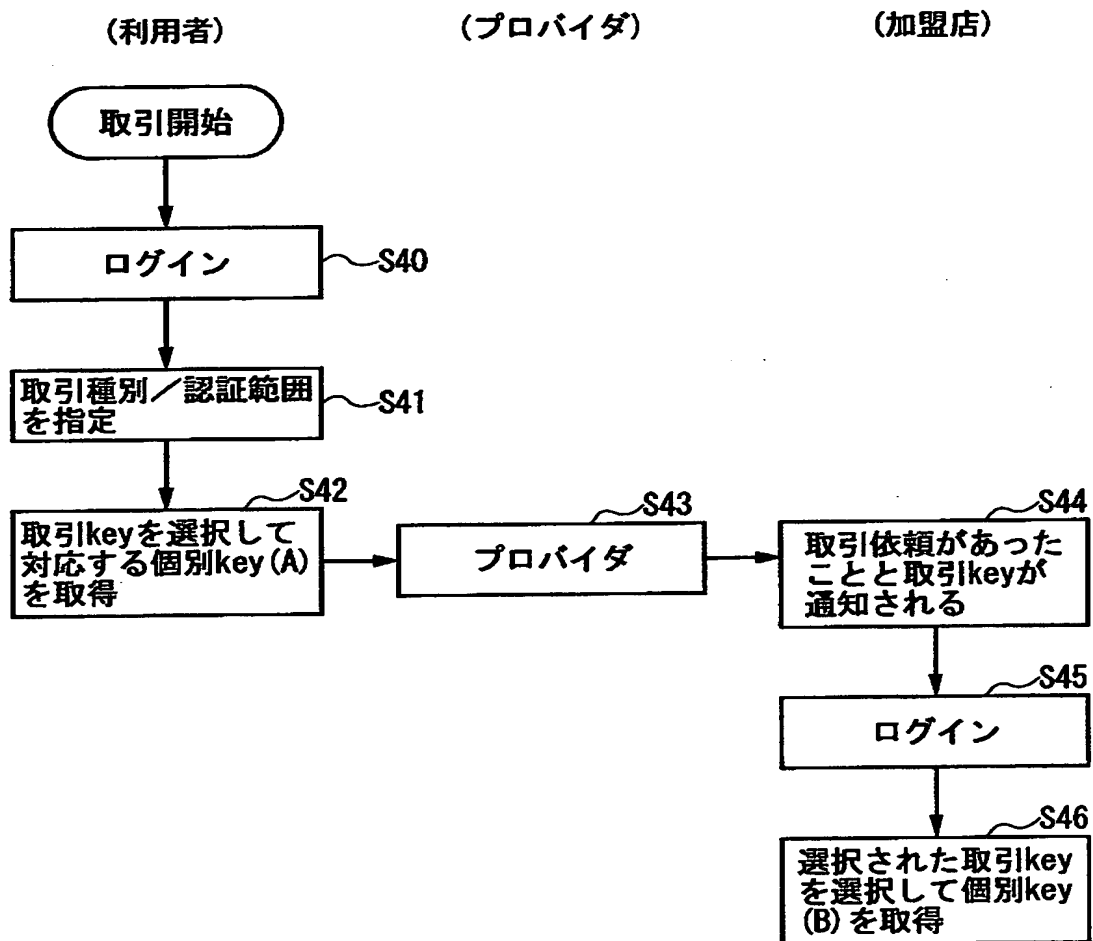
【図 5】

前処理の処理フローの例



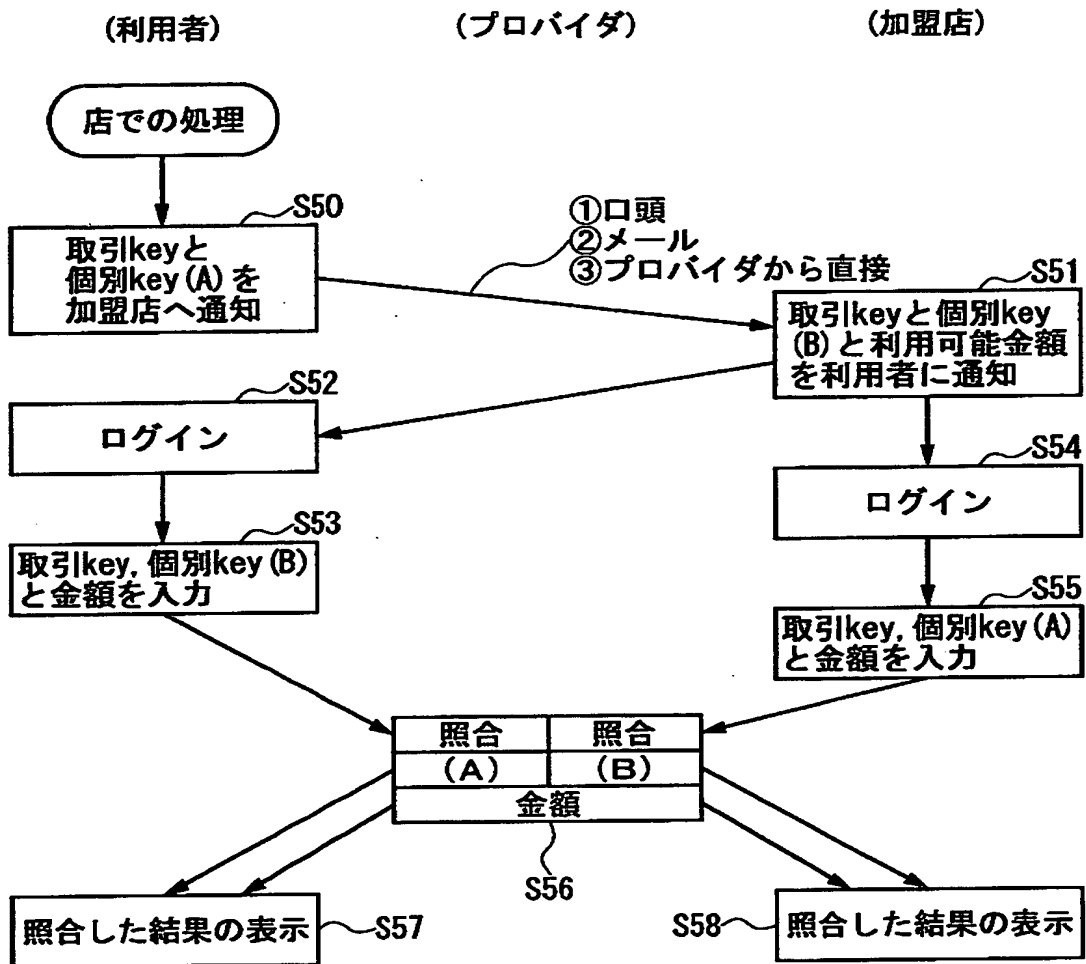
【図 6】

取引を開始して、レストランの利用者が
レストランに行くまでの処理フローの例



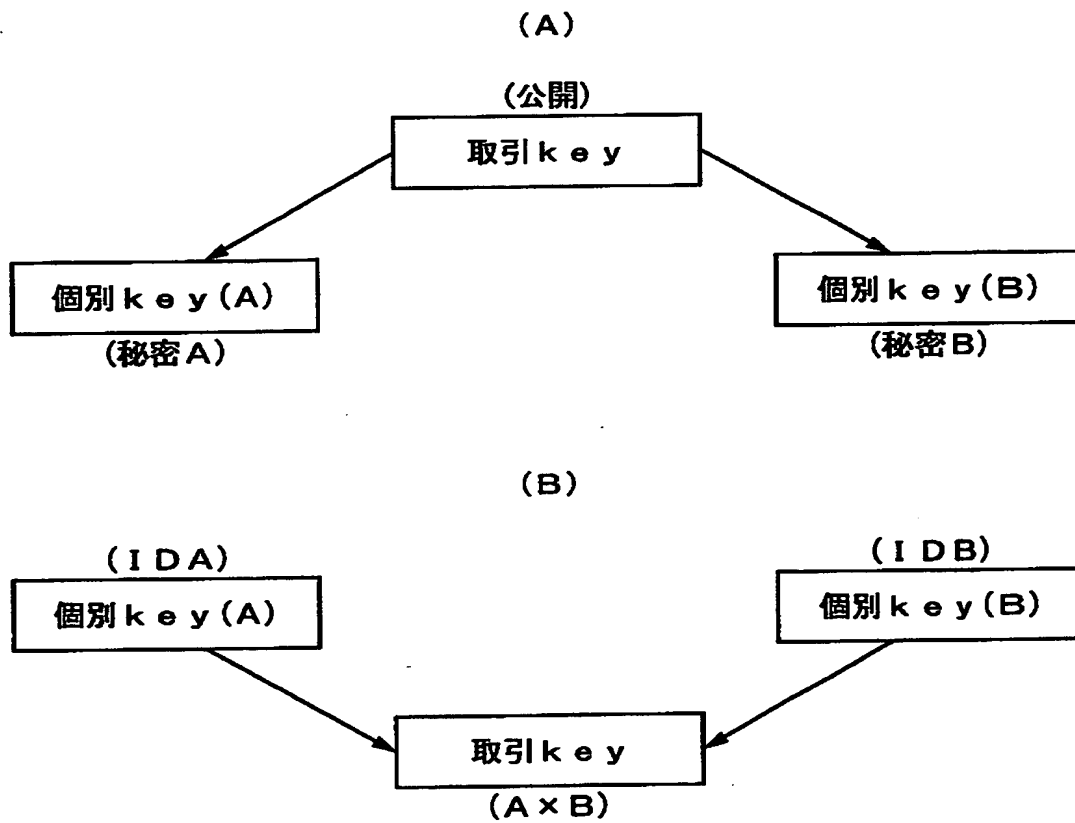
【図 7】

レストランの受付カウンターでの処理フローの例



【図 8】

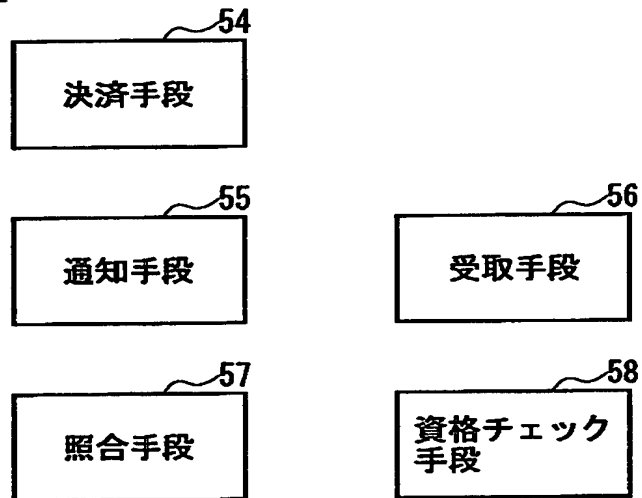
取引の照合を説明するための図



【図 9】

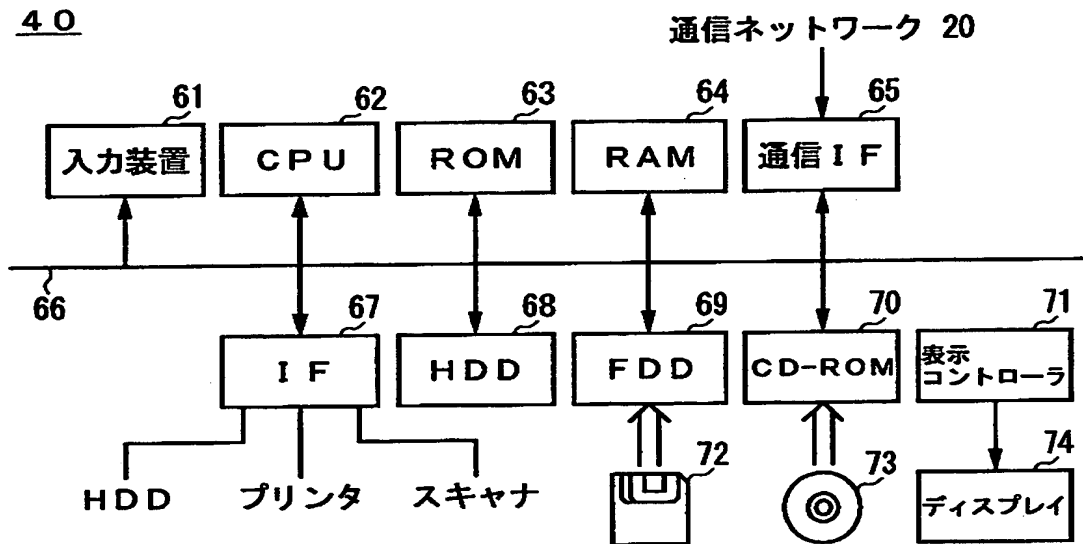
認証・決済システムにおける主要な機能ブロックの
例を説明するための図

4 1



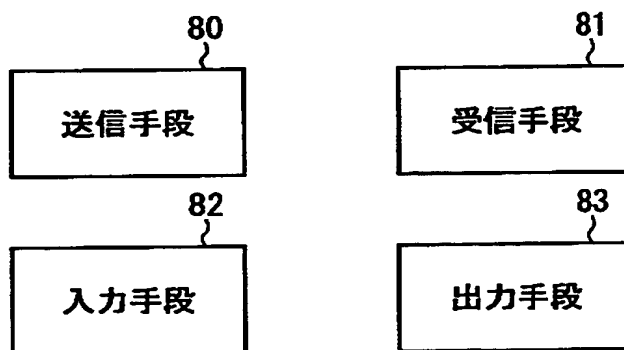
【図 1 0】

プロバイダのハードウェア構成の例を説明するための図



【図 1 1】

利用者端末(A, B)における
主要な機能ブロックの例を説明するための図



【書類名】 要約書

【要約】

【課題】 テンポラリな情報で認証を可能とし、安全で利便性の高い認証・決済手段を提供することを目的とする。

【解決手段】 初対面時に、利用者Bと、利用者Aとで認証を行う例である。予め、利用者Aと利用者Bは、プロバイダに登録する（S10）。対面したとき、個々の端末を用いて、本サービスが利用可能であること認証し（S11）、更に、取引資格の確認を行う（S12）。次いで、利用者Aと利用者Bは、同一の取引キーの選定を行い（S13）、プロバイダから、それぞれ、異なる照合キーを受ける（S14）。利用者Aと利用者Bは、その照合キーを交換し（S15）、相手から通知された照合キーを、プロバイダが提供する画面上で入力する（S16）。プロバイダは、照合キーの照合を行い（S17）、その結果を、利用者Aと利用者Bに通知する（S18）。その後、必要に応じて、決済する（S19）。

【選択図】 図2

出 願 人 履 歴 情 報

識別番号 [000005223]

1. 変更年月日 1996年 3月26日

[変更理由] 住所変更

住 所 神奈川県川崎市中原区上小田中4丁目1番1号

氏 名 富士通株式会社